DEPARTMENT OF THE ARMY
SEVENTH U.S ARMY JOINT MULTINATIONAL TRAINING COMMAND
UNIT 28130
APO AE 09114

AETT-IM

1 May 2007

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Information Assurance (Command Policy Letter 11)

1. References:

a. Army Regulation 25-1, Army Knowledge Management and Information Technology Management , 15 July 2005.

b. Army Regulation 25-2, Information Assurance, 14 November 2003.

c. Army in Europe Supplement 1 to Army Regulation 25-1, 28 April 2006.

d. Army in Europe Supplement 1 to Army Regulation 25-2, 30 June 2005.

2. There are internal and external threats, vulnerabilities and risks associated with our automated information systems. Operating systems, software applications, email, and hardware are all vulnerable, to attack. We must protect ourselves and our equipment from assailants that range from individual hackers to hostile foreign agencies.

3. Information Assurance (IA), a program that protects our systems against unauthorized access, modification of information, or denial of service, protects the integrity of our systems. Information Assurance is a commander's program and commanders must lead in establishing preventive measures.

a. Commanders and staff directors must ensure that everyone who uses a computer has proper access to the classification of that computer and understands the basic principles of Information Assurance and the security risks involved. Computer operators in the Seventh U.S. Army Joint Multinational Training Command (JMTC) must first pass the USAREUR Information Assurance Computer users licensing requirement and sign a computer-user agreement statement before using our computers.

b. Commanders and staff directors will ensure their IA staff is registered and has certification training documented into the Asset and Vulnerability Tracking Resource (A&VTR) database within 30 days of appointment. Failure to meet this requirement will result in revocation of a computer user's privileges.

c. Commanders and staff directors will ensure that their systems comply with the USAREUR Information Assurance configuration baselines on the Regional Computer Emergency Response Team, Europe (RCERT-E) website at https://iassure.usreur.army.mil. There are no authorized

peer-to-peer file sharing or communication tool sets authorized for use in the Army other than those provided by Army Knowledge Online (AKO). All instances where a user is using or has loaded a peer-to-peer implementation on a system will result in administrative and judicial actions for the user, and may include associated supervisors.

d. Users will maintain current anti-virus software and IAVA compliance on all systems at all times. Commanders and staff directors will ensure that all automated information systems meet and maintain information assurance baselines, and are formally accredited prior to being placed into operation. All systems will have an official risk assessment defined in the Department of Defense Information Technology Systems Accreditation and Certification Program (DITSCAP) before being turned on.

e. Commanders and staff directors must establish a clear hierarchy of Information Assurance appointment orders to ensure compliance with established objectives, policies, and directives as they pertain to the integrity, availability and confidentiality of automated information. The Information Assurance Manager (IAM) within the JMTC, G6 office is the executive agent for implementing Information Assurance in JMTC.

4. Information Assurance Vulnerability and Dragon Lightening alerts are issued by the G6 of the Army when there is a vulnerability that could result in administrator privilege compromise, effect a platform/system that is widely fielded, or effect critical Army systems or networks. JMTC offices are required to implement corrective measures within established suspense dates. When the G6 IAM disseminates alerts (via email), they have the same authority as an official tasking for all JMTC activities. **IA Staff reports acknowledgement of receipt and compliance to all IAVAs and IA Bulletins via the DA Information Assurance Database at https://newnewia.us.army.mil, the JMTC IAM will validate the status for the Command.**

5. Point of Contact for this policy is Mr. Ronnie Besco, email: Ronnie.besco@us.army.mil

DAVID R. HOGG
Brigadier General, U.S. Army
Commanding

DISTRIBUTION:
A